UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Seizure of *(Briefly describe the property to be seized)* All funds— including crypto-currency—stored in the Gemini Account associated to Account ID 61668, Group ID 1061668.	)	Case No. 2:21-mj-702

APPLICATION FOR A WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

I, a federal law enforcement officer or attorney for the government, request a seizure warrant and state under penalty of perjury that I have reason to believe that the following property in the Southern District of New York is subject to forfeiture to the United States of America under 18 U.S.C. § 981 & 982 *(describe the property)*:

All funds— including crypto-currency—stored in the Gemini Account associated to Account ID 61668, Group ID 1061668.

The application is based on these facts:

See Attached affidavit of support

❒ Continued on the attached sheet.

Gregory Libow

Applicant's signature

Gregory Libow

Printed name and title

Sworn to before me and signed in my presence.

Date: October 29, 2021

Kimberly A. Johnson
United States Magistrate Judge

City and state: Columbus, Ohio

AFFIDAVIT IN SUPPORT OF APPLICATIONS FOR SEIZURE WARRANTS

I, Gregory Libow, being duly sworn under oath, depose and say:

INTRODUCTION

1. I am a Special Agent with the HSI and have been since May of 2019. I am assigned to the Central Ohio Cyber Drug Taskforce (COCDTF) in Columbus, Ohio, where I am is responsible for conducting narcotics investigations involving dark web marketplaces. Prior to becoming a Special Agent, I was employed as a United States Customs and Border Protection (CBP) Officer for 8 years. While working for CBP, I was assigned to Columbus, Ohio and worked alongside HSI and other law enforcement agencies targeting drug and weapon shipments purchased off the internet. As a Special Agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States. Since working for HSI, I have been involved in narcotics-related arrests, executed search warrants that resulted in the seizure of narcotics, and participated in narcotics investigations. Through training and experience, I am familiar with the manner in which persons involved in the illicit distribution of controlled substances often operate.
2. Based on my training, experience, and participation in drug trafficking and computer-related investigations, I know and have observed the following:
    a. I have learned about the manner in which individuals and organizations distribute controlled substances throughout the United States;
    b. I know drug traffickers often purchase and/or title assets in fictitious names, aliases or the names of relatives, associates, or business entities to avoid detection of these assets by government agencies. I know that even though these assets are

in the names other than the drug traffickers, the drug traffickers actually own and continue to use these assets and exercise dominion and control over them;

c. I know drug traffickers must maintain on-hand large amounts of crypto-currency and U.S. currency to include stored in financial accounts readily accessible in order to maintain and finance their ongoing drug business;

d. I know when drug traffickers amass large proceeds from the sale of drugs, the drug traffickers attempt to legitimize these profits through money laundering activities. To accomplish these goals, drug traffickers utilize the following methods, including, but not limited to: domestic and international banks and their attendant services, securities brokers, professionals such as attorneys and accountants, casinos, real estate, shell corporations and business fronts and otherwise legitimate businesses which generate large quantities of currency; and

e. I know that Bitcoin and other crypto currency accounts are often times used by drug traffickers to launder money or conceal drug proceeds because of the anonymity associated with the use of Bitcoin and other crypto currency accounts and because crypto currency is decentralized.

PURPOSE OF AFFIDAVIT

3. This affidavit is submitted in support of an application for a combined criminal and civil forfeiture seizure warrant for all funds and digital currencies in the following Gemini Trust Company LLC account:

f. All remaining funds—including cryptocurrencies—stored in the Gemini Trust Company LLC belonging to Rex Devon TAYLOR, User ID 61838.

(collectively, hereafter, the "SUBJECT ACCOUNT").

4. As set forth below, I submit that there is probable cause to believe that the SUBJECT ACCOUNT is property constituting, or derived from, proceeds obtained, directly or indirectly, as a result of violations of 21 U.S.C. § 841 (To manufacture, distribute, or dispense a controlled substance) and 21 U.S.C. § 846 (conspiracy to distribute and possess with intent to distribute, controlled substances, including distribution by means of the Internet). The SUBJECT ACCOUNT is therefore subject to forfeiture to the United States under 21 U.S.C. § 853.

5. I further submit that there is probable cause to believe that the SUBJECT ACCOUNT constitutes (1) moneys, negotiable instruments, securities, or other things of value furnished or intended to be furnished in exchange for a controlled substance, in violation of the Controlled Substances Act ("CSA"); (2) proceeds traceable to such an exchange; or (3) moneys, negotiable instruments, or securities used or intended to be used to facilitate a violation of the CSA. The SUBJECT ACCOUNT is therefore subject to forfeiture to the United States under 21 U.S.C. § 881(a)(6).

6. Additionally, there is probable cause to believe that the SUBJECT ACCOUNT constitutes property involved in a money laundering transaction or money laundering conspiracy, in violation of 18 U.S.C. § 1956, or are traceable to such property. The SUBJECT ACCOUNT is, therefore, subject to forfeiture to the United States pursuant to 18 U.S.C. §§ 981(a)(1) (civil forfeiture) and 982(a)(1) (criminal forfeiture).

7. Because this affidavit is submitted for the limited purpose of obtaining warrants authorizing the seizure of the SUBJECT ACCOUNT, I am not including every fact known to me about DEFENDANT or the larger investigation.

8. This affidavit is based upon my own personal observations, my training and experience, discussions with other agents who are familiar with this investigation, and information collected during this investigation through, among other things, witness interviews, law enforcement investigation reports, information obtained through searches, and public records.

FORFEITURE AND SEIZURE AUTHORITY

9. As to civil forfeiture, under 21 U.S.C. § 881(a), "[t]he following shall be subject to forfeiture to the United States and no property right shall exist in them: . . . (6) All moneys, negotiable instruments, securities, or other things of value furnished or intended to be furnished by any person in exchange for a controlled substance or listed chemical in violation of this subchapter, all proceeds traceable to such an exchange, and all moneys, negotiable instruments, and securities used or intended to be used to facilitate any violation of this subchapter." Property subject to civil forfeiture under 21 U.S.C. § 881(a) may be seized pursuant to 18 U.S.C. § 981(b) (by 21 U.S.C. § 881(b)). Under 18 U.S.C. § 981(a)(1)(A), "[a]ny property, real or personal, involved in a transaction in violation of [18 U.S.C. §§ 1956], or any property traceable to such property" is subject to forfeiture to the United States. Property subject to civil forfeiture under 18 U.S.C. § 981(a)(1) may be seized pursuant to 18 U.S.C. § 981(b).

10. As to criminal forfeiture, under 21 U.S.C. § 853(a), "[a]ny person convicted of a violation of this subchapter or subchapter II of this chapter punishable by imprisonment for more than one year shall forfeit to the United States, irrespective of any provision of State law [*inter alia*]—(1) any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; [and] (2) any of the

person's property used, or intended to be used, in any manner or part, to commit, or to facilitate the commission of, such violation." As property subject to criminal forfeiture under 21 U.S.C. § 853(a), the SUBJECT ACCOUNT may be seized pursuant to 21 U.S.C. § 853(f). Under 21 U.S.C. § 970, Section 853 applies in every respect to a violation of this subchapter punishable by imprisonment for more than one year, including violations of 21 U.S.C. § 963.

11. Under 18 U.S.C. § 982(a)(1), "[t]he court, in imposing sentence on a person convicted of an offense in violation of 18 U.S.C. §§ 1956 shall order that the person forfeit to the United States any property, real or personal, involved in such offense, or any property traceable to such property." As property subject to criminal forfeiture under 18 U.S.C. § 982(a)(1), the SUBJECT ACCOUNT may be seized pursuant to 21 U.S.C. § 853(f) (by 18 U.S.C. § 982(b)(1).

12. With respect to seizure, 21 U.S.C. § 853(f) specifically provides that a court may issue a criminal seizure warrant when it "determines that there is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture and that a[] [protective] order under [21 U.S.C. § 853(e)] may not be sufficient to assure the availability of the property for forfeiture." As set forth further below, there is a substantial risk that the SUBJECT ACCOUNT will be withdrawn, moved, dissipated, or otherwise become unavailable for forfeiture unless immediate steps are taken to secure them. As a form of cryptocurrency, the SUBJECT ACCOUNT is inherently portable and fungible. I therefore submit that a protective order under 21 U.S.C. § 853(e) would not be sufficient to assure that the SUBJECT ACCOUNT will remain available for forfeiture.

13. Furthermore, pursuant to 18 U.S.C. § 981(b)(3), "[n]otwithstanding the provisions of rule 41(a) of the Federal Rules of Criminal Procedure, a seizure warrant may be issued pursuant to this subsection by a judicial officer in any district in which a forfeiture action against the property may be filed under section 1355(b) of title 28, and may be executed in any district in which the property is found, or transmitted to the central authority of any foreign state for service in accordance with any treaty or other international agreement."

14. For the reasons listed above, the United States seeks a combined criminal and civil seizure warrant, authorizing law enforcement to seize the SUBJECT ACCOUNT and preserve it pending further forfeiture proceedings.

BACKGROUND ON THE DARK WEB & CRYPTOCURRENCY

15. Based on my training, research, education, and experience, I am familiar with the following relevant terms and definitions:

a. The "dark web" is a portion of the "deep web[1]" of the Internet, where individuals must use an anonymizing software or application called a "darknet" to access content and websites. Within the dark web, criminal marketplaces operate, allowing individuals to buy and sell illegal items, such as drugs, firearms, and other hazardous materials, with greater anonymity than is possible on the traditional Internet (sometimes called the "clear web" or simply the "web"). These online market websites use a variety of technologies, including the Tor network (defined below) and other encryption technologies, to ensure that communications and transactions are shielded from

[1] The deep web is the portion of the Internet not indexed by search engines. Examples are databases and internal networks belonging to private industry, government agencies, or academic institutions.

interception and monitoring. Famous dark web marketplaces ("DWM's"), also called Hidden Services, such as Silk Road 1, Silk Road 2, AlphaBay, and Hansa (all of which have since been shut down by law enforcement), operated similarly to clear web commercial websites such as Amazon and eBay, but offered illicit goods and services. When law enforcement shut down the four DWM's listed above, they also obtained images of their servers, and law enforcement has been able to mine the data from those sites for information about the customers and vendors who used them.

b. "Vendors" are the dark web's sellers of goods and services, often of an illicit nature, and they do so through the creation and operation of "vendor accounts" on dark web marketplaces. Customers, meanwhile, operate "customer accounts." Vendor and customer accounts are not identified by numbers, but rather monikers or "handles," much like the username one would use on a clear web site. If a moniker on a particular marketplace has not already been registered by another user, vendors and customers can use the same moniker across multiple marketplaces, and based on seller and customer reviews, can become well known as "trusted" vendors or customers. It is also possible for the same person to operate multiple customer accounts and multiple vendor accounts at the same time. For example, based on my training and experience, I know that one person could have a vendor account that he or she uses to sell illegal goods on a dark web marketplace in exchange for cryptocurrency; that same vendor could also have a different customer account that he or she uses to exchange cryptocurrency earned from vendor sales for fiat currency[2]. Because they are separate accounts, a person could use different

[2] Fiat currency is currency created and regulated by a government such as the U.S. Dollar, Euro, or Japanese Yen.

accounts to send and receive the same cryptocurrency on the dark web. I know from training and experience that one of the reasons dark web vendors have multiple monikers for different vendor and customer accounts, is to prevent law enforcement from identifying which accounts belong to the same person, and who the actual person is that owns or uses the accounts.

c. The "Tor network," or simply "Tor" (an abbreviation for "The Onion Router"), is a special network of computers on the Internet, distributed around the world, designed to conceal the true Internet Protocol ("IP") addresses of the computers accessing the network, and, thereby, the locations and identities of the network's users. Tor also enables websites to operate on the network in a way that conceals the true IP addresses of the computer servers hosting the websites, which are referred to as "hidden services" on the Tor network. Such hidden services operating on Tor have complex web addresses, generated by a computer algorithm, ending in ".onion" and can only be accessed through specific web browser software, including a browser known as "Tor Browser," designed to access the Tor network. Examples of hidden services websites are the aforementioned AlphaBay and Hansa. Tor is available on cellphones using the Android and Apple operating systems by installing an application that puts a TOR-enabled internet browser on a user's cellphone, which then routes the phone's IP address through different servers all over the world, making it extremely difficult to track.

d. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrency are Bitcoin, Litecoin, and Ether. Cryptocurrency can exist

digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.[3] Cryptocurrency is not illegal in the United States.

e. Bitcoin[4] ("BTC") is a type of cryptocurrency. Payments or transfers of value made with bitcoin are recorded in the Bitcoin blockchain and thus are not maintained by any single administrator or entity. As mentioned above, individuals can acquire bitcoin through exchanges (i.e., online companies which allow individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), bitcoin ATMs, or directly from other people. Individuals can also acquire cryptocurrencies by "mining." An individual can "mine" bitcoins by using his/her computing power to solve a complicated algorithm and verify and record payments on the blockchain. Individuals are rewarded for this task by receiving newly created units of a cryptocurrency. Individuals can send and receive cryptocurrencies online using many types of electronic devices,

[3] Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

[4] Since Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted practice is to use "Bitcoin" (singular with an uppercase letter B) to label the protocol, software, and community, and "bitcoin" (with a lowercase letter b) to label units of the cryptocurrency. That practice is adopted here.

including laptop computers and smart phones. Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that individual or entity. Bitcoin transactions are therefore sometimes described as "pseudonymous," meaning that they are partially anonymous. And while it's not completely anonymous, Bitcoin allows users to transfer funds more anonymously than would be possible through traditional banking and credit systems.

f. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or "public key") and the private address (or "private key.") A public address is represented as a case-sensitive string of letters and numbers, 26–25 (35) characters long. Each public address is controlled and/or accessed through the use of a unique corresponding private key - the cryptographic equivalent of a password or PIN - needed to access the address. Only the holder of an address' private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

g. Although cryptocurrencies such as Bitcoin have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as

money laundering and is an oft-used means of payment for illegal goods and services on hidden services websites operating on the Tor network. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track purchases within the dark web marketplaces. As of October 27, 2021, one bitcoin is worth approximately $59,000.00, though the value of bitcoin is generally much more volatile than that of fiat currencies.

h. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (e.g. Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR code[5] with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a "recovery seed" (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency

[5] A QR code is a matrix barcode that is a machine-readable optical label.

wallets can include two-factor authorization (such as a password and a phrase). I also know that individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

i. Bitcoin "exchangers" and "exchanges" are individuals or companies that exchange bitcoin for other currencies, including U.S. dollars. According to the Department of Treasury, Financial Crimes Enforcement Network ("FinCEN") Guidance issued on March 18, 2013, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services businesses.[6] Such exchanges and exchangers are required to register with FinCEN and have proper state licenses (if required under applicable state law). From my training and experience, I know that registered money transmitters are required by law to follow Bank Secrecy Act anti-money laundering ("AML") regulations, "Know Your Customer" ("KYC") protocols, and other verification procedures similar to those employed by traditional financial institutions. For example, FinCEN-registered cryptocurrency exchangers often require customers who want to open or maintain accounts on their exchange to provide their name, address, phone number, and/or the full bank account and routing numbers that the customer links to his/her exchange account. As a result, there is significant market demand for illicit cryptocurrency-for-fiat currency exchangers, who not only lack AML or KYC protocols but often advertise their ability to offer customers stealth and anonymity. These illicit exchangers often exchange fiat currency for cryptocurrencies, such as by meeting

[6] *See* "Application of FinCEN's Regulations to Person Administering, Exchanging, or Using Virtual Currencies," *available at* https://www.fincen.gov/resources/statutes-regulations/guiadance/application-fincens-regulations-persons-administering.

customers in person or by shipping fiat currency through the mail. Due to the illicit nature of these transactions and their customers' desire for anonymity, such exchangers are frequently able to charge a higher exchange fee, often as high as 9-10% (in contrast to registered and BSA-compliant exchangers, who may charge fees as low as 1-2%).

j. Some companies offer cryptocurrency wallet services which allow users to download a digital wallet application onto their smart phone or other digital device. A user typically accesses the wallet application by inputting a user-generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the application; however, many of these companies do not store or otherwise have access to their users' funds or the private keys that are necessary to access users' wallet applications. Rather, the private keys are stored on the device on which the wallet application is installed (or any digital or physical backup private key that the user creates). As a result, these companies generally cannot assist in seizing or otherwise restraining their users' cryptocurrency. Nevertheless, law enforcement could seize cryptocurrency from the user's wallet directly, such as by accessing the user's smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet (see above), investigators may be able to use the recovery seed phrase to recover or reconstitute the wallet on a different digital device and subsequently transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet.

PROBABLE CAUSE STATEMENT

SUMMARY OF THE INVESTIGATION

16. On October 04, 2019 the Central Ohio Cyber Drug Taskforce (COCDTF) in Columbus, Ohio, consisting of investigators assigned to HSI, Drug Enforcement Administration (DEA), United States Postal Inspection Service (USPIS) and the Internal Revenue Service (IRS), executed a federal search warrant at a Columbus, Ohio Target's residence, who was using an online moniker to purchase narcotics off the Darknet site Empire Market. Investigators found and seized computers, cypto-currency, U.S. currency, firearms, and controlled substances from the residence. Analysis of the Columbus Target's Darknet Empire Market account, indicated that he had been communicating with and purchasing liquid psychedelic mushrooms from an online vendor using the Darknet moniker "TRIPWITHSCIENCE" on a regular basis.

17. Open source research determined that "TRIPWITHSCIENCE" had operated on several Darknet markets since approximately 2011, totaling over 17,000 transactions: Empire Market (4,719 transactions), Agora (1,500 transactions), Apollon Market (47 transactions), Berlusconi Market (60 transactions), Cryptonia Market (199 transactions), Dream Market (6,400 transactions), Tochka Market (542 transactions), Hansa Market (567 transactions), Silk Road 2.0 (2,199 transactions) and Dark Market (823 transactions). The research also indicated that "TRIPWITHSCIENCE" may have operated on Nightmare Market, Andromeda Market, AlphaBay, Silk Road, Wall Street Market, Pandora, Black Market Reloaded, and numerous other small Darknet markets, but the number of transactions associated with those markets is unknown. "TRIPWITHSCIENCE" additionally operated on Monopoly, Televend and Cannahome Darknet marketplaces selling liquid psychedelic mushrooms in 9.0 milligram/gram vials for $19.95 each. "TRIPWITHSCIENCE" specifically stated how to consume the

controlled substance on his marketplace listings, verifying the controlled substance analogue is for human consumption.

18. From December 23, 2019 through November 20, 2020, HSI Columbus, with assistance from DEA and USPIS, conducted twelve (12) controlled liquid mushroom buys from "TRIPWITHSCIENCE" via Empire and Cannahome Markets. HSI Columbus purchased a total of approximately 545 grams of liquid psychedelic mushrooms during the twelve buys. HSI received and seized a U.S. Mail parcel associated with each buy containing suspected liquid psychedelic mushrooms. The Ohio Bureau of Criminal Investigation (BCI) Forensic Laboratory tested the contents of each parcel and determined them to be 4-Acetoxy-N,N-Dimethyltryptamine (4-AcO-DMT). This controlled substance is an analogue of 4-Hydroxy-N,N-Dimethyltryptamine (liquid psychedelic mushrooms), a schedule I controlled substance.

19. On or about October 22, 2020, HSI Columbus received data from a seized Darknet Marketplace that contained 34 Bitcoin withdrawal wallet addresses for "TRIPWITHSCIENCE's" vender account. Using cryptocurrency analysis tracing, a Coinbase wallet was discovered sending and receiving Bitcoin from "TRIPWITHSCIENCE's" withdrawal wallets. A subpoena was served to Coinbase for the subscriber information and account history associated with the Coinbase customer conducting the bitcoin transactions. Coinbase subpoena returns revealed the user account, created on January 22, 2013, belonged to James BARLOW.

20. While reviewing seized Darknet Marketplace data from "TRIPWITHSCIENCE," HSI SAs discovered messages between "TRIPWITHSCIENCE and Darknet moniker "DARKLOIS." The messages identified "DARKLOIS" as a shill account created by

"TRIPWITHSCIENCE" to promote his business and create test shipments on his account. Agents discovered a similar conversation between "DARKLOIS" and Darknet vendor "PERFECTSHROOMS," the only other account "DARKLOIS" reviewed and interacted with. HSI Agents identified two additional shill Darknet buyer accounts, "APPLETITS" and "BOTTLEWHISKEYSHL," being used by "TRIPWITHSCIENCE" and "PERFECTSHROOMS" to promote their sales on multiple Darknet marketplaces including Hansa Market. "PERFECTSHROOMS" had listings on Televend, Monopoly and Cannahome marketplaces. The account had listings for 3.5 grams to 114 grams of "Organic Mushrooms" (Psilocybe Cubensis Shrooms) in capsule form. A February 14, 2020 Established Vender Application stated PerfectShrooms had processed 7,800 orders on 15 different darknet marketplaces.

21. An investigative search conducted on the darknet website Empire Market for the vendor "TRIPWITHSCIENCE" revealed a listing for "Liquid Mushrooms (Pure Psilocybin Extract)." The listing advertised vials of approximately 9mg of "Liquid Mushrooms" for $19.95 each. The listing allowed buyers to purchase in unlimited quantities/increments. This search revealed "TRIPWITHSCIENCE," who was active on the market from December 3, 2018 through November 23, 2019, had completed 2,555 transactions. There were 1,732 positive feedback comments left for "TRIPWITHSCIENCE" during that time frame, which regularly commented on the quality of the product.

22. On November 30, 2020, HSI Special Agent Gregory Libow obtained a search warrant for the Google account of James BARLOW, JIM.V.BARLOW@GMAIL.COM. Numerous items of evidentiary value were located indicating Rex TAYLOR is associated with the TRIPWITHSCIENCE DTO:

A. On April 14, 2013, BARLOW emailed Rex TAYLOR, REXTAYLOR@Q.COM, an email titled, "The Dark Internet". In the email BARLOW wrote, "Have you heard about this? http://gawker.com/5805928/ In that article they mention bitcoins - it's like an anonymous version of cash you can send to anyone anywhere in the world. It's really cool." A clearweb search of the link sent by BARLOW redirected to an article titled, "The Underground Website Where You Can Buy Any Drug Imaginable".

B. On April 3, 2014, TAYLOR sent an email titled, "myco". In the email TAYLOR wrote, "More pizza topping" and attached numerous images of TAYLOR holding and eating mushrooms. Rex TAYLOR sent an additional email titled, "Silly sighbin". In the email TAYLOR wrote, "Those were the days" and attached numerous images of mushrooms growing in mason jars. "Silly sighbin" is believed to be slang for Psilocybin Mushrooms. METADATA????

C. On July 20, 2014, BARLOW received an email from Coinbase titled, "You just sent 0.40 BTC to Rex Taylor". The content of the email stated, "Hi Jim B, You just sent 0.40 BTC (worth $250.22 USD) to Rex Taylor. Attached message: For week 1, July 14-20". This payment is consistent with payments BARLOW sent TAYLOR for his involvement in the TRIPWITHSCIENCE DTO, as detailed on a "1 Orderman BTC" payment sheet for payments to TAYLOR.

D. On October 5, 2014, BARLOW, DROPBOX@JIMBARLOW.NET, received an email from Dropbox titled, "Rex Taylor joined your shared folder". The content of the email stated, "Hi Jim, Rex Taylor joined your shared folder ".lwt"!" Per records obtained during a search warrant of BARLOW's Dropbox account, the folder associated with "lwt" contained numerous documents associated with the TRIPWITHSCIENCE DTO.

E. On January 22, 2015, BARLOW sent an email to Rex TAYLOR, REXTAYLOR@Q.COM, titled, "Linux Mint usb". The content of the email stated, "If you can get Linux Mint running from ANY usb stick, we can recreate everything. All of the necessary files were backed up in the LWT folder - right? So even if the original stick is toast, we didn't lose anything."

F. On April 29, 2015, BARLOW received an email from Dropbox titled, "Rex Taylor joined your shared folder". The content of the email stated, "Hi Jim, Rex Taylor joined your shared folder "DNM-Files"!" DNM-Files are believed to be files associated with the darknet market activity of TRIPWITHSCIENCE.

G. On May 2, 2015, BARLOW received an email titled, "Receipt for Your Payment to FlashRouters.com" from Paypal, service@paypal.com. The content of the email stated, "Shipping address – confirmed Rex Taylor **5011 N 2800 W Cedar City, UT 84721** United States" for "PrivateInternetAccess Cisco Linksys E1200 DD-WRT FlashRouter Item# E1200-PIA-E1200-FLASH-SUPPORT-BASIC-3MONTH-90DAY". Investigators know FlashRouters were purchased by BARLOW and sent to DTO members to the locations DTO members facilitated their drug trafficking. FlashRouters were used to hide the true VPN of DTO members when processing orders from the darknet for the TRIPWITHSCIENCE DTO.

H. On October 15, 2015, BARLOW sent a message to TAYLOR, "Don't know if you're in cell range, but I'm taking care of orders today, so you're good until Saturday. Hope you're having fun!" TAYLOR replied, "I really appreciate it I'll catch things up on Saturday".

I. On a screenshot image, saved as "Screenshot_20190618-102556", a screenshot was saved of a list of things to do. The image listed, "tws NIGHTMARE order checks",

"openbazaar listing", "ob2 service restarter", "where tochka $ going?????", "email team about orderman 1 ordeal", "spreadsheet Calc commission & currency". Investigator's know ORDERMAN1 is a moniker used by TAYLOR, TWS is short for TRIPWITHSCIENCE, and TRIPWITHSCIENCE sold on NIGHTMARE and TOCHKA darknet markets.

23. Also in the records associated with JIM.V.BARLOW@GMAIL.COM were multiple spreadsheets referencing Darknet marketplaces and bitcoin transactions believed to be sales ledgers for "TRIPWITHSCIENCE" and "PERFECTSHROOMS." In a spreadsheet titled "2015 TCS Accounting" were 9 tabs, 7 of the tabs were titled 2015 and contained known two letter abbreviations for darknet markets AlphaBay, Nucleus Market, Abraxas Market, MiddleEarth Marketplace, Evolution Market, Agora Market and Black Bank Market. A tab titled "2015 Received" appeared to list all 704 Darknet transactions from January 1, 2015 through December 9, 2015. A second spreadsheet titled "TCS Accounting." showed tabs for each year from 2014 to 2021 and a summary tab. Each tab dated for a certain year showed a detail ledger. Many of the ledgers included references to Darknet marketplaces, bitcoin mixing services and drug transactions. The summary tab broke down each year's net, average month, average day, and total bitcoins earned for the year. A third spreadsheet titled "TWS Sales Summation" was found by investigators on BARLOW's Google Drive in a folder named "DNM," known by law enforcement to be an abbreviation for Darknet Market. The spreadsheet showed a sales ledger for Liquid Mushrooms sold in July of 2014 on Silk Road, Agora and Evolution Darknet markets. The ledger claimed, at the time, the TRIPWITHSCIENCE DTO was averaging 682 orders a month and selling approximately 2,555 vials per month.

24. On April 21, 2021, James BARLOW and additional co-conspirators were arrested for warrants issued by the Southern District of Ohio for Conspiracy to Possess with Intent to Distribute Psychedelic Mushroom Analogue.

25. On April 29, 2021, a proffer session of a Cooperating Defendant, herein referred to as CD1, was held. During the proffer session, CD1 stated TAYLOR, AKA: "ORDERMAN1", AKA: 1 ORDERMAN, AKA: ORDERMAN, was hired to assist him/her with the TRIPWITHSCIENCE DTO. CD1 stated TAYLOR would scrape orders from the darknet markets and send the labels and orders to the shippers to fill. CD1 stated TAYLOR additionally grew mushrooms for the DTO from late 2015 or 2016 until 2017. CD1 indicated he/she used these psilocybin mushrooms to create his liquid mushroom extract for sale. CD1 additionally stated TAYLOR had access to the TRIPWITHSCIENCE darknet accounts and to the darknet market withdraw wallets.

26. On May 5, 2021, Agent Libow reviewed darknet wallet addresses obtained from an encrypted hard drive / hidden folder on James BARLOW's computer seized during BARLOW's arrest on April 21. SA Libow reviewed a document saved as "1 Orderman BTC" in folder employee>payments>archived. The "1 Orderman BTC" document contained multiple items of evidentiary value detailing amounts of packages/vials shipped and transactions paid to TAYLOR each month for his involvement in the TRIPWITHSCIENCE and PERFECTSHROOMS DTOs. The ledger represented payments from TRIPWITHSCIENCE/PERFECTSHROOMS DTOs to TAYLOR from December 2014 through June 2019 and totaled 172.839600 BTC in payments. The 172 BTC is currently valued at approximately $10,500,000. The funds paid to TAYLOR on the ledger included his salary and miscellaneous payments for "Thumb Drive

Reimbursement", "vials shipped", "days scraping", and other involvement by TAYLOR to further his drug trafficking for the DTO. The ledger is not believed to be all inclusive and is not believed to include all packages and vials shipped by TAYLOR, nor orders TAYLOR scraped from darknet markets to process orders for other drug shippers. Agent Libow was able to review an additional spreadsheet located on BARLOW's computer which calculated the average sales per day/month of the TRIPWITHSCIENCE and PERFECTSHROOMS DTOs. Investigators were able to determine TAYLOR worked approximately 55 months for the TRIPWITHSCIENCE DTO in which the members were responsible for approximately 2,335 kilograms of drugs trafficked. Additionally, investigators were able to determine TAYLOR worked approximately 16 months for the PERFECTSHROOMS DTO in which members were responsible for approximately 134 kilograms of drugs trafficked.

27. The "1 Orderman BTC" document specifically detailed a payment on May 15, 2017 to TAYLOR, labeled "Orderman May 15 Salary", for $1,200/.68 BTC to address 1E4qLDHe7LSjcutjapguq6jWN4XPUKjTbH. This ledger further listed the Bitcoin (BTC) address 1FaeEgnHwXu99vz3ZgfgWDSSATuabDdTCp attributed to TAYLOR. On June 8, 2021, Gemini Trust Company, LLC was served Subpoena IB-21-301798 for the subscriber information and account history of the user associated with the Gemini Trust Company account associated with wallet address 1FaeEgnHwXu99vz3ZgfgWDSSATuabDdTCp. On June 17, Gemini Trust Company, LLC subpoena returns revealed the wallet address 1FaeEgnHwXu99vz3ZgfgWDSSATuabDdTCp was attributed to Gemini Trust Company user Rex TAYLOR. Subpoena returns further showed TAYLOR received 0.6801092

BTC on May 15, 2017 to address 1E4qLDHe7LSjcutjapguq6jWN4XPUKjTbH via transaction hash 8a679bb2b0356c7d3cb65cec45bb987469a570128db78d9c542f5ca1a6a04172. This transaction is congruent with the transaction detailed in the "1 Orderman BTC" payment ledger. Records showed during the life of the account, TAYLOR deposited 15.56043304 BTC into the account and withdrew $123,832.67. Many of the transactions were similar to amounts / payment dates as the transactions detailed on the "1 Orderman BTC" sheet. The returns further listed the email address: REXTAYLOR@Q.COM.

28. On June 4, a proffer session of a second Cooperating Defendant, herein referred to as CD2, was held. During the proffer session CD2 admitted in 2014, BARLOW asked his uncle, Rex TAYLOR, to be an "orderman". CD2 explained he/she and BARLOW went to TAYLOR's residence in Utah, where BARLOW taught TAYLOR and CD2 how to be a "shipper" and an "orderman" for the TRIPWITHSCIENCE DTO. CD2 stated BARLOW created a spreadsheet system to log: orders, order problems, amounts of drugs sent, profits, and market access information. CD2 stated BARLOW went to Utah numerous times to fix TAYLOR's computer. CD2 stated BARLOW would also remote into TAYLOR and his/her computer when they had computer related issues. CD2 stated around 2016 to 2018, TAYLOR continued to be an "orderman". CD2 stated they believed once TAYLOR made enough money to purchase an airplane from his drug earnings with TRIPWITHSCIENCE he stepped away from the DTO. CD2 indicated "ORDERMAN" or "ORDERMAN1" was a moniker used by TAYLOR for the TRIPWITHSCIENCE DTO. CD2 stated an "orderman" was paid approximately $2,000 to $4,000 a month depending on the number of days worked. CD2 stated an "orderman"

would be responsible for handling customer disputes on the markets and would occasionally speak with the darknet market moderators.

29. On August 5, a proffer session of a third Cooperating Defendant, herein referred to as CD3, was held. CD3 stated after January of 2018 he/she and Matthew BARLOW received customers' order details and addresses from TAYLOR and would mix and ship the drugs in priority mail envelopes and stamps. CD3 stated when he/she and Matthew BARLOW began working for TRIPWITHSCIENCE, TAYLOR and another individual were the only employees that were currently working for the TRIPWITHSCIENCE DTO. CD3 informed investigators that they believed in July of 2019, TAYLOR stopped working for the DTOs and he/she and Matthew BARLOW took over TAYLOR's job of downloading orders from Darknet Marketplaces.

30. On August 31, a proffer interview of a fourth Cooperating Defendant, herein referred to as CD4, was conducted. CD4 told investigators that Rex TAYLOR was an "orderman" and indicated sometime during the first quarter of 2018, trained CD4 to perform that job.

31. On October 6, HSI Special Agent (SA) Libow conducted blockchain analysis on bitcoin payment addresses used by the TRIPWITHSCIENCE DTO, including the bitcoin (BTC) wallet bc1qd6sqv05v67njrzqxvv7xryptgc2mycs0wsus5q named "share dividends orderman1" which was found on James BARLOW's hidden SINK drive folder. The "share dividends orderman1" wallet is believed to belong to TAYLOR, AKA: ORDERMAN1. Blockchain analysis showed TAYLOR received continual "shared dividend" payments from the TRIPWITHSCIENCE DTO until the co-conspirator arrests on April 21, 2021.

32. On May 10, 2021, a "share dividends orderman1" wallet sent the .10833 BTC to another wallet address where it was combined with an additional 8.76378 BTC, valued at approximately $504,063.71, which came from several wallets which also received their funds from Wasabi Mixer. As of October 14, 2021, the 8.87211 BTC remains in the second wallet. Investigators believe TAYLOR is likely in control of the funds contained in the second wallet containing 8.87211 BTC.

33. On October 13, an arrest warrant was issued by the Honorable Chelsey M. Vascura for TAYLOR in the United States District Court for the Southern District of Ohio for: 21 U.S.C. Section 841 - Knowingly or intentionally attempt to manufacture, distribute, or dispense, or possess with intent to manufacture, distribute, or dispense a controlled substance and 21 U.S.C Section 846 - Attempt and conspiracy to commit an act in violation of 21 U.S.C. Section 841. On October 19, TAYLOR was arrested.

34. On October 20, a telephone interview was conducted with TAYLOR. During the interview TAYLOR explained to investigators that in 2014 he was down on his luck and began working for the TRIPWITHSCIENCE (TWS) drug trafficking organization (DTO). TAYLOR stated that he agreed to work for the DTO under the condition that they only sell psilocybin mushrooms. TAYLOR stated that he worked for the TWS DTO from 2014 until late 2017. TAYLOR said that once he stopped working for TWS, he continued to receive small dividend payouts in Bitcoin. TAYLOR stated that he noticed the payments disappeared approximately six months ago.

35. Records were obtained from Gemini Trust Company, LLC for the account of TAYLOR. Records showed TAYLOR last logged into his account on October 5, 2021 from IP address 199.167.89.65. Records show TAYLOR's account holds a balance of

1.25178654 BTC worth approximately $71,264. Records further showed TAYLOR's account previously had two deposits from Hydra Marketplace and two deposits "with medium paths" from Dream Market and Agora darknet marketplaces.

LAUNDERING OF NARCOTICS PROCEEDS AND ANALYSIS OF CRYPTOCURRENCY INTO THE SUBJECT ACCOUNT

36. Transactions on DWMs such as those described in this affidavit are conducted through the use of cryptocurrency, primarily Bitcoin, in order to facilitate anonymity. Proceeds from transactions on DWMs are deposited to a common wallet within the DWM known as a "hot wallet," and available balances are tracked within each user account. When a vendor wants to withdraw funds from the DWM, he/she withdraws Bitcoin from his/her DWM "account" to a Bitcoin address within his/her control. Bitcoin from the hot wallet is then transferred to the address indicated by the vendor. These financial transactions, conducted with the proceeds of illegal narcotics sales, were executed with the knowledge that it would conceal the nature, source, and origin, of such proceeds, constituting money laundering transactions under 18 U.S.C. § 1956.

37. To obtain fiat value from cryptocurrency, it must be exchanged from Bitcoin to the individual's fiat currency of choice (e.g., USD, GBP, or some denomination). This transformation of value occurs at cryptocurrency exchanges, such as Gemini, Celsius, Binance, Kraken, BlockFi, or other like exchanges, which are money services businesses (MSBs). In order to use an exchange, an individual must create an account at the exchange and then send Bitcoin, or other form of cryptocurrency, from an address they control to an address associated with their account at the cryptocurrency exchange. The individual could then withdraw funds from the cryptocurrency exchange to their bank of choice; alternately, it could be exchanged for other forms of cryptocurrency (e.g.,

Ethereum, Litecoin, etc.). Conducting financial transactions with the proceeds of illegal narcotics sales with the knowledge that it would conceal their nature, source, and origin, e.g., converting pseudonymous bitcoin proceeds into seemingly legitimate fiat currency, constitutes money laundering under 18 U.S.C. § 1956.

38. Because of the nature of how bitcoin is transferred between addresses, tracing a bitcoin transaction is akin to tracking a serialized dollar through the financial system. As a result, it is impractical to employ traditional tracing methods to complex, multi-hop bitcoin transactions. Instead, bitcoin flow analysis shows the overall path of where bitcoin came from prior to reaching a certain wallet or address. So, while the activity may not be directly traceable at the transactional level, it can often be indirectly traced back to an origin wallet or address. Because every bitcoin transaction is entered into the public blockchain ledger, investigators can use historical blockchain analysis to determine which origin wallets belong to bitcoin addresses well-known to law enforcement, such as DWMs (e.g., Silk Road 1, Hansa, etc.), exchanges (e.g., Celsius, Binance, Kraken, BlockFi, etc.), or peer-to-peer exchange platforms (e.g., LocalBitcoins). Wallets and addresses that belong to unknown individuals, however, are far more difficult to identify.

39. After conducting blockchain analysis, investigators believe the Gemini Trust Company, LLC identified is controlled by Rex TAYLOR. A portion of the funds deposited into the wallet appeared to originate from darknet markets and mixing services used to mask the transfer funds.

40. Very few, if any, of the products/services being sold on DWMs are legal (e.g., contraband such as heroin) or are being sold legally (e.g., illegal sales of prescription drugs). Therefore, bitcoins being withdrawn from the DWM's represents proceeds of

illegal activity in nearly every instance. Because the bitcoins being withdrawn from the DWM's consist almost entirely of criminal proceeds, I submit there is probable cause to seize the 1.25178654 BTC remaining in TAYLOR's Gemini Trust Company, LLC account.

SEALING REQUEST

41. It is respectfully requested that the Court issue an order sealing, until further order of the Court, all papers submitted in support of the requested seizure warrant, including the application, this affidavit, and the requested search warrant. I believe that sealing these documents is necessary because the information to be seized is relevant to an ongoing investigation. Premature disclosure of the contents of the application, this affidavit, and the requested seizure warrant may adversely affect the integrity of the investigation, including giving TAYLOR a chance to destroy evidence or take other steps to hinder the investigation. Furthermore, because of the confidential nature of law enforcement analysis techniques disclosed herein, sealing is critical. Dark web vendors and other criminals in the dark web space frequently search the internet for legal process that describes current law enforcement techniques for tracing cryptocurrency and identifying dark web vendors. As a result, sealing this request is critical for countless ongoing investigations around the country.

Gregory Libow

Special Agent Gregory Libow
Homeland Security Investigations

Sworn to before me on
October 29, 2021

Kimberly A. Johnson
United States Magistrate Judge

ATTACHMENT A

All funds— including crypto-currency—stored in the Gemini Account associated to Account ID 61668, Group ID 1061668.